IN-16POEWM

User Manual

16 Port Fast Ethernet

PoE Web Smart Switch

Version V100817

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Content	1
Introduction	2
Hardware Description	5
User Log In	7
Administrator	8
Port Management	13
VLAN Setting	17
Per Port Counter	21
QoS Setting	22
Security	24
Spanning Tree	26
Trunking	29
Backup/Recovery	30
Miscellaneous (IGMP)	31
Logout	32

Introduction

Product Overview

This 16 ports 10/100 Mbps PoE web-smart switch includes auto-MDI/MDIX crossover detection function. 16 of those ports are all built with PoE functionality, providing the ultimate choice in network flexibility. With this added PoE feature, this switch is an ideal solution for building wireless, IP surveillance, and VoIP networks.

This 16 ports web-smart PoE switch provides a port-based and 802.1Q tag VLAN function to provide better traffic management, reduce latency, improve security and save bandwidth. This is also a cost-saving feature as it reduces the need to add additional hardware to the network.

The switch has 16 10/100BASE-TX ports that support the IEEE 802.3af PoE protocol. Each port and transmit a maximum power 15.4 watts. User can also enable or disable power supply on PoE ports from UI.

Web Management Features

- Port Management
  Port Configuration
  Port Mirroring
  Bandwidth Control
  Broadcast Strom Control
  PoE On/Off Setting

- VLAN Setting
  Port-based/ Tag-based
  VLAN ID: 1~4094

- Trunking
  Link Aggregation Setting
  2 groups (1~4 port for each group)

- QoS Setting
  Priority Mode
  Class of Service Configuration
  TCP/UDP Port-based

- Security Setting
  MAC address filtering

TCP/UDP Port filtering

- STP/RSTP
- Spanning Tree Protocol
- Backup Recovery Configuration

Specifications

- Standard

  IEEE 802.3 10BaseT
  IEEE 802.3u 100BaseTX
  IEEE 802.ab 1000BaseT
  IEEE 802.3z 1000BaseSX/LX
  IEEE 802.3x Full-duplex and Flow Control
  IEEE 802.af PoE
  IEEE 802.3ad Link Aggregation
  IEEE 802.1d Spanning tree protocol
  IEEE 802.1w Rapid Spanning tree protocol
  IEEE 802.1x Port-based Network Access Control
  IEEE 802.1Q VLAN
  IEEE 802.1p Class of Service

- Number of Port

  16-port 10/100BaseTX with PoE (Full power)

Mechanical

- LED Indicator

  Per Port: Link/ Act
  PoE Port: Act/Status
  Per Unit: Power

- Power Consumption: 260Watts (Max)
- Power Input: 100~240V/AC, 50~60HZ
- Power Output: 48V/DC per Port Output – 15.4W Max per Port
- Product Dimensions/ Weight

  44 × 220 × 440 mm (H × W ×D) / 3.1kg

Performance

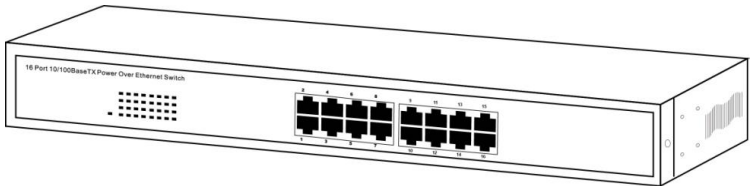
- MAC Address: 4K

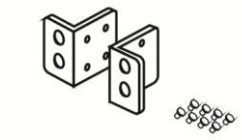
- Buffer Memory: 1.625Mb
- Transmission Method: Store and Forward

Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- One Fast Ethernet PoE Switch
- One EU Power Cord
- A User Manual CD
- Rack-mount Kit





Hardware Description

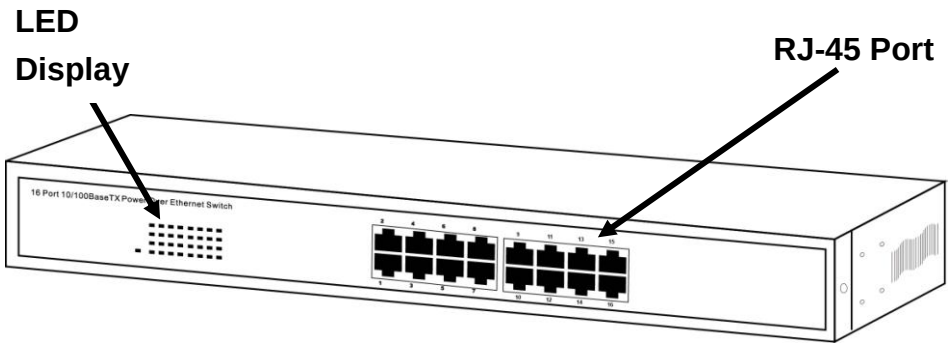
This section mainly describes the hardware of the 8 PoE port Ethernet Combo Web-Smart Switch and gives a physical and functional overview on the certain switch.

Physical Dimensions/ Weight

44 × 220 × 440 mm (H × W ×D) / 3.1kg

Front Panel

The front Panel of the Web Managed Switch consists of 16 10/100Base-TX RJ-45 ports. The LED Indicators are also located on the front panel.

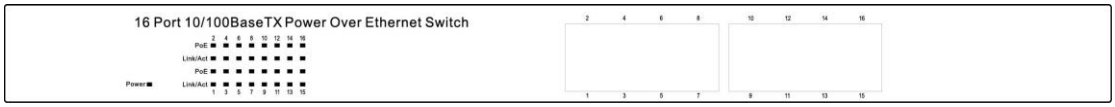


LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

Table 1-1 LED Indicators

LED	Status	Description
Power	On	Power is on.
	Off	Power is off.
	Blink	Reset Button for 3 seconds
PoE	On	Port is Linked to Power Device
	Off	No Power Device is connected
Link/Act	On	The port works in 10/100M
	Blinks (continuously)	Networking is active
	Off	No device attached



Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.

Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation. The last, use twisted pair cable to connect this switch to your PC then user could start to operate the switch.

User Log In

This part instructs user how to set up and manage the switch through the web user interface. Please follow the description to understand the procedure.

At the first, open the web browser, and go to 192.168.2.100 site then the user will see the login screen. Key in the password to pass the authentication then clicks the **OK**. The log in process is completed and comes out the sign “Password successfully entered”.

Log in

ID: admin

Password: admin

Figure 1-1

※Note: It will show error message if you key in wrong user name or password.

Figure 1-2

Main Page

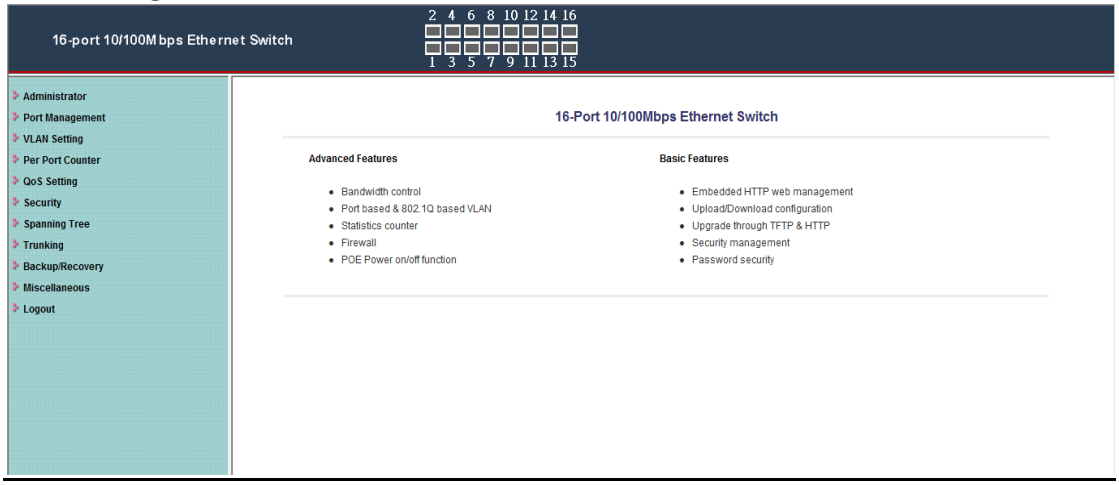


Figure 1-3

Administrator

Authentication Configuration

This page shows authentication configuration information. User can set new Username and Password in this page.

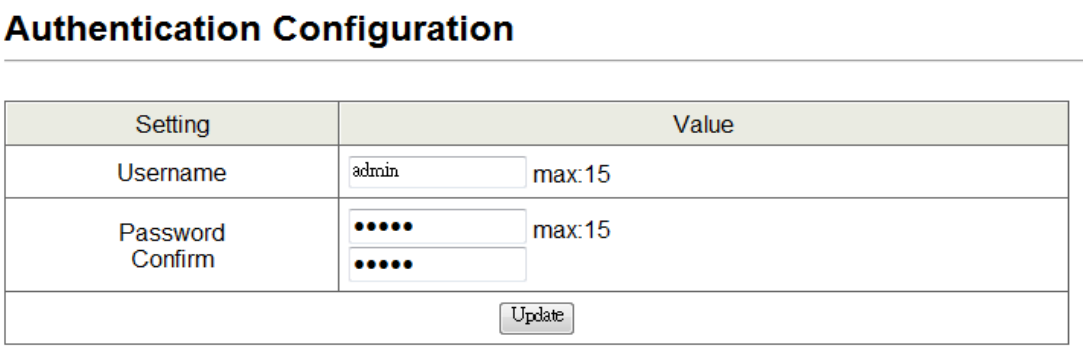


Figure 2-1

System IP Configuration

This page shows system configuration including the current IP address and sub-net mask and gateway.

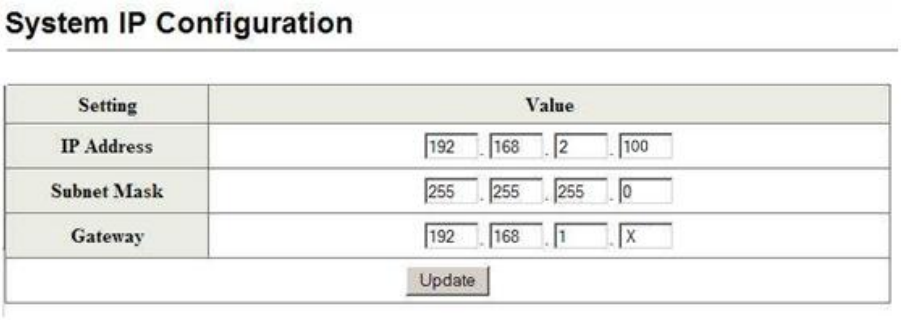


Figure 2-2

User can configure the IP settings, Subnet Mask, Gateway as below:

- IP address: Manually assign the IP address that the network is using. The default IP is 192.168.2.100
- Subnet Mask: Assign the subnet mask to the IP address.
- Gateway: Assign the network gateway for industrial switch. The default gateway is 192.168.2.254

If you change the IP address of this switch and then press **Update**. It will show "**update successfully**" then press **Reboot** button. It will enter user login screen automatically

System Status

This page displays the information about the switch of MAC address, how many ports it has, system version and. Besides, users can also fill in up to 15 characters in the Comment, Contact and Location field for note.

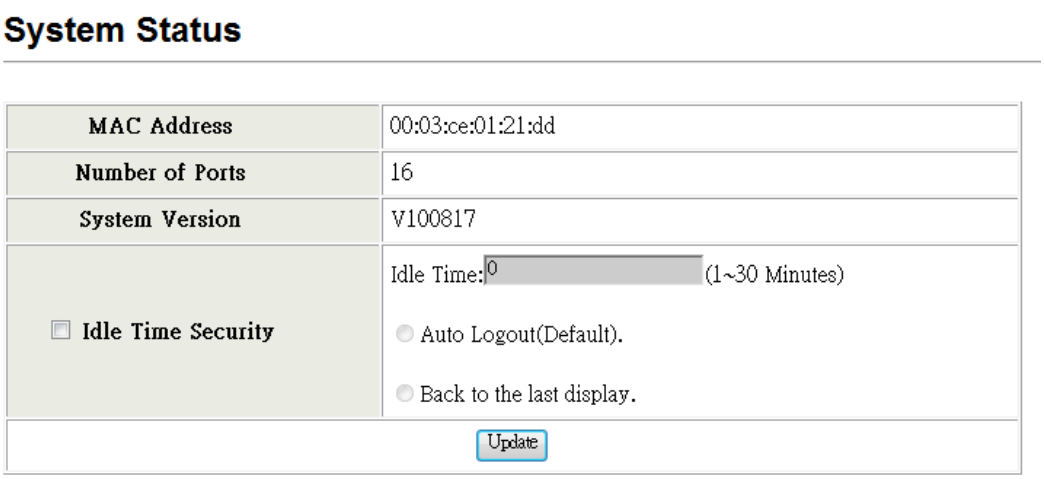


Figure 2-3

- MAC Address: Displays the unique hardware address assigned by manufacturer (default).
- Number of Ports: Displays number of ports in the switch.
- System Version: Displays the switch's firmware version.

- Idle Time Security: User can set the time security. When user leave the computer for a moment, the software will auto logout or back to the last display.

And then click **Update** button.

Load Default Setting

Clicking the **Load** button will make the switch being set to the original configuration.

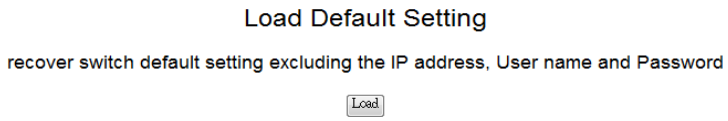


Figure 2-4

※ Note: It exclude to change user name, password and IP configuration. If you want to restore default setting including IP and user name password, then you can press the reset button for hardware base reset.

More detail information about Load Default Setting - Hardware Base is described as following.
The purpose of this function is to provide a method for the network administrator to restore all configurations to the default value.
(1) To activate this function, the user should follow the following procedures. Press the “Load default” button for 3 seconds until you see the LED blinking.
(2) When LED starts blinking, it means the CPU is executing the “load default” procedure. You can release the button now.
After completing this procedure, all the factory default value will be restored. It includes the IP address, the user name, the password and all switch configurations.

Firmware Update

Before the firmware update procedure is executed, you should enter the password twice and then press **Update** button. The smart switch will erase the flash memory. There is a self-protection mechanism in the Boot Loader, so the Boot Loader will keep intact. Even though the power is turned off or the cable link fails during the firmware update procedure, the Boot loader will restore the code to firmware update page.

Firmware Update
Please input the password to continue the Firmware Update process.
Password
ReConfirm
Update
Notice:After clicking the "UPDATE" button, IF the firmware update webpage is not redirected correctly or is shown as "Webpage not found". Please connect to http://192.168.2.100

Figure 2-5

After pressing Update button, the old web code will be erased. Then you can select the image file and press “update” button to update the firmware you need.

Firmware Update by Web
Select the image file:
Browse...
UPDATE
If the update process somehow goes wrong(Ex: power failure), please connect to http://192.168.2.1 to restart.(If possible, reset device first.)
Firmware Update by TFTP
(TFTP client)Use MS Windows' Command Prompt window to run tftp client program.
Syntax: c:\tftp -i 192.168.1.1 put FILE_DIRECTORY\FILENAME.bin

Figure 2-6

Reboot Device

Click **Confirm** button to reboot the device.

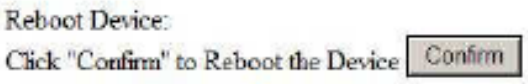


Figure 2-7

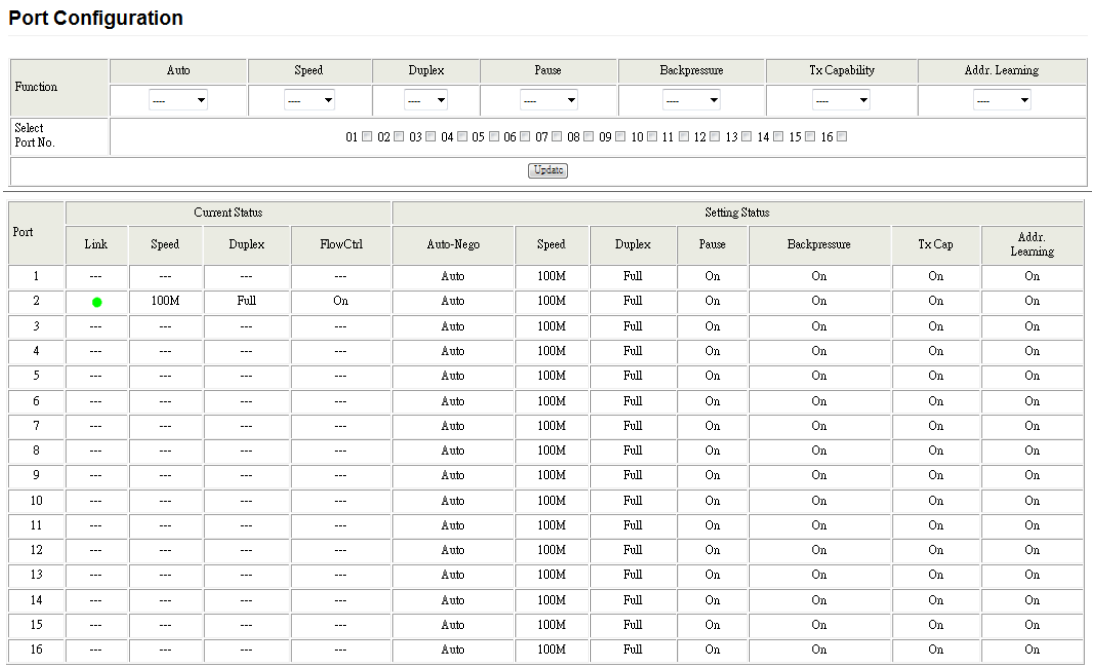
※Note: The reboot is for software base instead of hardware base.

Port Management

Port Management includes Port Configuration, Port Mirroring, Bandwidth Control, Broadcast Storm Control and PoE

Port Configuration

In Port Configuration, you can set and view the operation mode for each port.



Port Configuration

Function	Auto	Speed	Duplex	Pause	Backpressure	Tx Capability	Addr. Learning
	---	---	---	---	---	---	---

Select Port No. 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

Update

Port	Current Status				Setting Status						
	Link	Speed	Duplex	FlowCtrl	Auto-Nego	Speed	Duplex	Pause	Backpressure	Tx Cap	Addr. Learning
1	---	---	---	---	Auto	100M	Full	On	On	On	On
2	●	100M	Full	On	Auto	100M	Full	On	On	On	On
3	---	---	---	---	Auto	100M	Full	On	On	On	On
4	---	---	---	---	Auto	100M	Full	On	On	On	On
5	---	---	---	---	Auto	100M	Full	On	On	On	On
6	---	---	---	---	Auto	100M	Full	On	On	On	On
7	---	---	---	---	Auto	100M	Full	On	On	On	On
8	---	---	---	---	Auto	100M	Full	On	On	On	On
9	---	---	---	---	Auto	100M	Full	On	On	On	On
10	---	---	---	---	Auto	100M	Full	On	On	On	On
11	---	---	---	---	Auto	100M	Full	On	On	On	On
12	---	---	---	---	Auto	100M	Full	On	On	On	On
13	---	---	---	---	Auto	100M	Full	On	On	On	On
14	---	---	---	---	Auto	100M	Full	On	On	On	On
15	---	---	---	---	Auto	100M	Full	On	On	On	On
16	---	---	---	---	Auto	100M	Full	On	On	On	On

Figure 3-1

- Auto-Negotiation: Enable and Disable. Being set as ‘Enable’, the Speed, Duplex mode, Pause, Backpressure, TX Capability and Address Learning are negotiated automatically. When you set it as ‘Disable’, you have to assign those items manually.
- Speed: When the Auto-Negotiation column is set as Disable, users have to set the connection speed to the ports ticked.
- Duplex: When the Auto-Negotiation column is set as Disable, users have to set the connection mode in Half/Full to the ports ticked.
- Pause: Flow Control for connection at speed of 10/100Mbps in Full-duplex mode.
- Backpressure: Flow Control for connection at speed of 10/100Mbps in Half-duplex mode.
- TX/RX Capability: When the Auto-Negotiation column is set as Disable, users have to set this column as Enable or Disable.
- Addr. Learning: When the Auto-Negotiation column is set as Disable, users have to set this column as Enable or Disable.

- Select Port No.: Tick the check boxes beside the port numbers being set.
- Click Update to have the configuration take effect.
- Current Status: Displays current port status.
- Setting Status: Displays current status.

Click **Update** to make the configuration effective.

Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. That Traffic through ports can be monitored by any of the ports means traffic goes in or out monitored (source) ports will be duplicated into mirroring (destination) port.

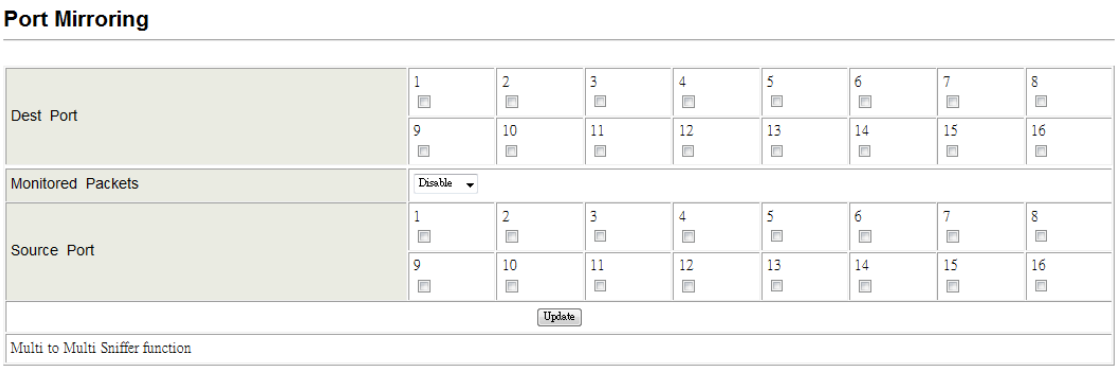

Port Mirroring
Dest Port
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Monitored Packets
Disable
Source Port
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Update
Multi to Multi Sniffer function

Figure 3-2

- Destination (mirroring) port for monitoring Rx only, Tx only or both RX and TX traffic which come from the source port. Users can connect the mirroring port to LAN analyzer or Netxray.
- Monitored Packets: Pull down the selection menu to choose what kind of packet is to be monitored.
- Source Port: The ports that the user wants to monitor. All monitored port traffic will be copied to mirroring (destination) port. Users can select multiple source ports by ticking the check boxes beneath the port number label to be monitored.

And then, click **Update** to have the configuration take effect.

Bandwidth Control

This page allows the setting of the bandwidth for each port. The TX rate and Rx rate can be filled with the number ranging from 1 to 255. This number should be multiplied by the selected bandwidth resolution to get the actual bandwidth.

Bandwidth Control

Port No	Tx Rate Value	Rx Rate Value
01	Bandwidth = X resolution. (0~19/195/255) 0: Full speed. 1~19/195/255: Specified bandwidth.	Bandwidth = X resolution. (0~19/195/255) 0: Full speed. 1~19/195/255: Specified bandwidth.
Resolution	Low Low:32Kbps (1).Rate value: 1~255. High:512Kbps (1).When link speed is 10M and the resolution is 512Kbps, the Rate value should be 1~19. (2).When link speed is 100M and the resolution is 512Kbps, the Rate value should be 1~195. All ports use the same bandwidth resolution.	
Update LoadDefault		
If the link speed of selected port is lower than the rate that you setting, this system will use the value of link speed as your setting rate.		

Port No	Tx Rate(Kbps)	Rx Rate(Kbps)	Link Speed	Port No	Tx Rate(Kbps)	Rx Rate(Kbps)	Link Speed
1	Full Speed	Full Speed	---	9	Full Speed	Full Speed	---
2	Full Speed	Full Speed	100M	10	Full Speed	Full Speed	---
3	Full Speed	Full Speed	---	11	Full Speed	Full Speed	---
4	Full Speed	Full Speed	---	12	Full Speed	Full Speed	---
5	Full Speed	Full Speed	---	13	Full Speed	Full Speed	---
6	Full Speed	Full Speed	---	14	Full Speed	Full Speed	---
7	Full Speed	Full Speed	---	15	Full Speed	Full Speed	---
8	Full Speed	Full Speed	---	16	Full Speed	Full Speed	---

Figure 3-3

Broadcast Storm Control

The switch implements a broadcast storm control mechanism. Tick the check boxes to have them beginning to drop incoming broadcast packets if the received broadcast packet counts reach the threshold defined. Each port's broadcast storm protection function can be enabled individually by ticking the check boxes.

Broadcast Storm Control

Threshold	63 1~63							
Enable Port	1	2	3	4	5	6	7	8
	9	10	11	12	13	14	15	16
Update								
This value indicates the number of broadcast packet which is allowed to enter each port in one time unit. One time unit is 500 us for 100Mbps speed and 5000us for 10Mbps speed								

Figure 3-4

The broadcast packet is only checked at the selected port and the number of broadcast packets is counted in every time unit. One time unit is 500 us for 10Mbps speed and 5ms for 100Mbps. The excessive broadcast packet will be discarded. For those broadcast packets incoming from the un-selected port, the switch treats it as the normal traffic.

- Threshold: Type in the threshold in the range between 1 and 63 to limit the maximum byte counts, which a port can send or receive in a period of time.
- Enable Port: Having ticked the boxes, the port will stop transmitting or receiving data when their sending byte counts or receiving byte counts

reach the defined threshold.

Click **Update** to have the configuration take effect.

PoE

User could know per PoE port out power status in this page and also enable or disable per port.

POE Configuration

Port	01	02	03	04	05	06	07	08
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Minimun Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---
Port	09	10	11	12	13	14	15	16
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Minimun Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---

Update

Update: Update the power control funtion.
Enable ☑ :Power On
Enable ☐ :Power Off

Figure 3-5

VLAN Setting

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

VLAN Mode

You may select the VLAN Mode of the switch. Port-based VLAN is for separating traffic only on this single switch. There is no handover of network traffic within VLAN groups to other switches. For the handover to other switches use Tag Based VLAN. In VLAN Mode you can switch from Tag to Port Based VLAN. Port Based VLAN is the default mode.

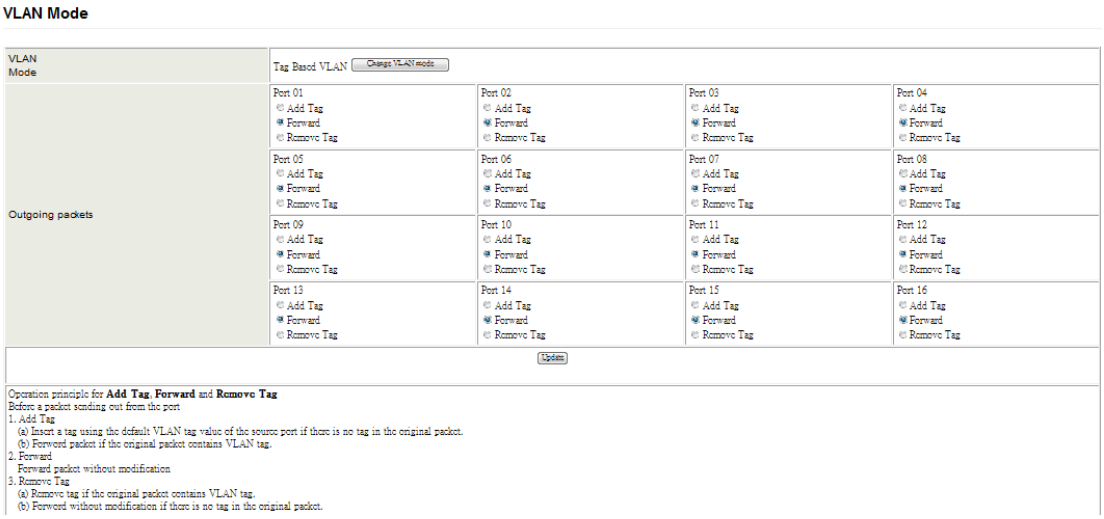


Figure 4-1

After having switched to Tag Based VLAN Mode, the screen changes. On this screen you can now define and configure your Up- and Downlink ports. These are important since here the handover between the switches of your network takes place.

Figure 4-2

- VLAN Mode: Displays VLAN mode: port based/Tag based VLAN. Here you can also switch back to Port Based VLAN Mode

- Add tag means the outgoing packet of the selected port will be inserted a 802.1Q tag. Use this setting for your Up- and Downlink Ports in your VLAN Tagged Network.
- Don't care means the outgoing packet of the selected port keep the original packet received at the source port.This is the default setting when starting VLAN configuration. You should change to either Add or Remove Tag.
- Remove tag means the 802.1Q tag of the outgoing packet of the selected port will not be sent. Use this setting for your Network Connections to PCs. Only packets of the VLAN Group the Port is member of will be sent.

VLAN Member

The ports need to be made member of your VLAN groups. This is for Tag Based and Port Based VLAN Mode. The screen here looks different whether you run Tag Based or Port Based Mode.

VLAN Member in Port Based Mode

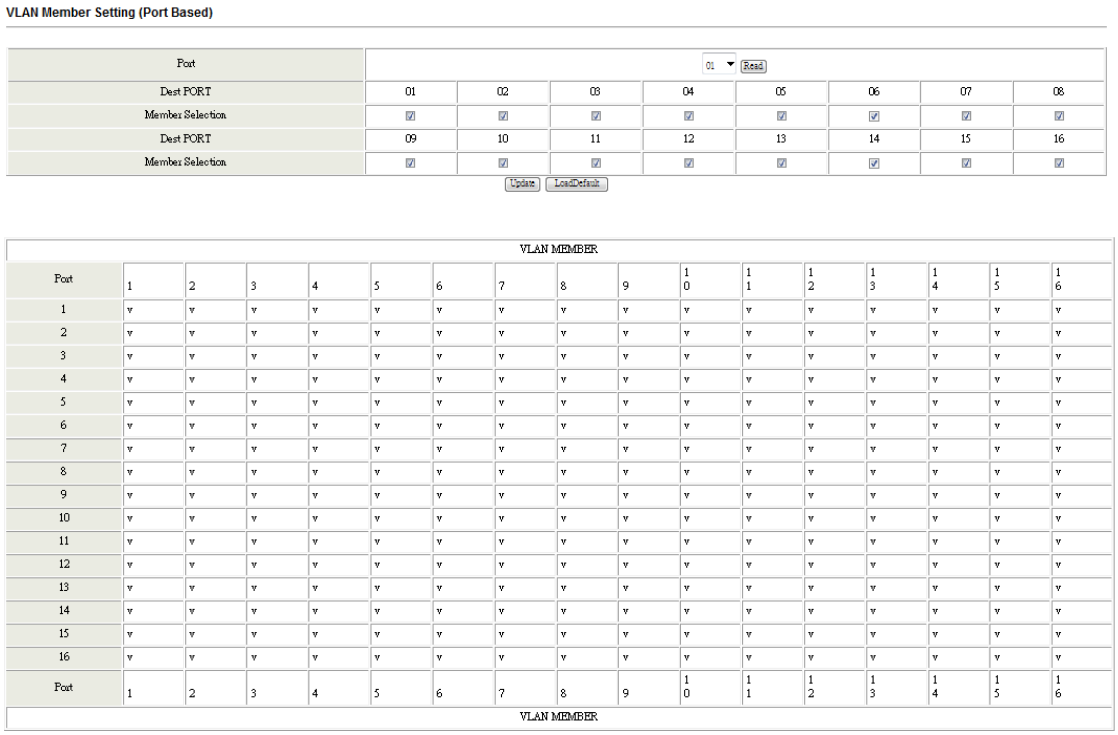


Figure 4-3

In Port Based Mode you see a matrix of your 8 Ports. Simply select the port on top screen you want to configure, click on Read, and then select or deselect the ports that are on the same VLAN group. In this configuration mode you do not need to worry about defining VLAN groups and VLAN IDs.

VLAN Member in Tag Based Mode

In Tag Based Mode you need to define and configure your VLAN groups. Since you want the handover to other switches take place smoothly, the VLAN IDs (Numbers) need to be like on the rest of your network. On other switches you may have the chance to configure names. These are just for your reference. Only the numbers are important!
There firstly add your VLAN Groups (identified throughout your network by unique and constant numbers). Start with IDs from 100 and up. Keep in mind that some switches use “1” as the default, while others use “4095” or “4096” as default. Starting with 100 gives you enough free room and less compatibility issues.

So enter “100” in the field right of VID Setting, then select or deselect which ports are member of that group. Your up- and downlink ports need to member of every existing group! Then click on add. The new group with its setting will be displayed at the bottom of the screen.

With the PVID Setting you define to which VLAN group incoming traffic belongs. Consider the example that Port 1 is member of group 100 and 101. A simple PC is connected to Port 1. If that PC is now sending out data, with PVID you define if that data is for group 100 or 101.

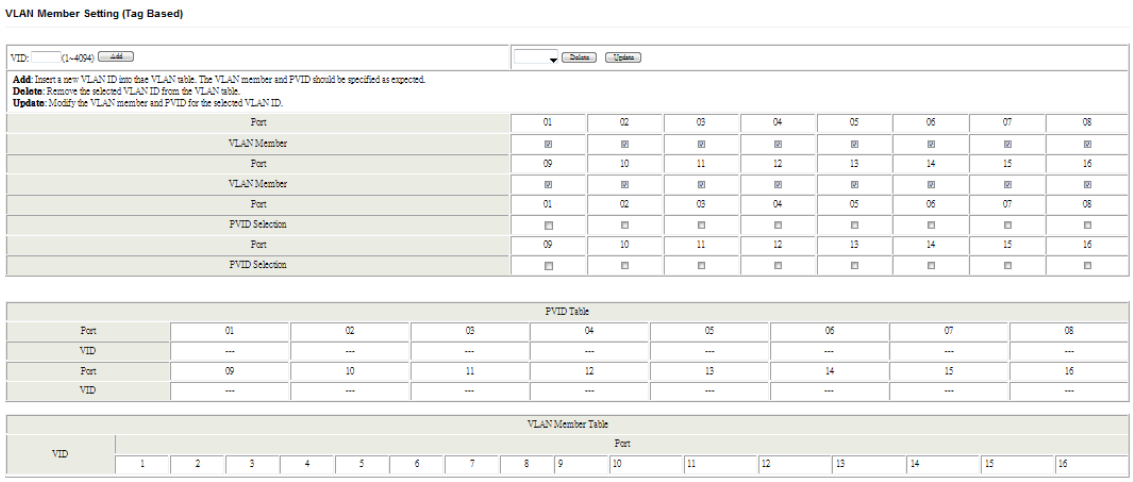

VLAN Member Setting (Tag Based)
VID: (1~4094) Add
Delete Update
Add: Insert a new VLAN ID into the VLAN table. The VLAN member and PVID should be specified as expected.
Delete: Remove the selected VLAN ID from the VLAN table.
Update: Modify the VLAN member and PVID for the selected VLAN ID.
Port 01 02 03 04 05 06 07 08
VLAN Member
Port 09 10 11 12 13 14 15 16
VLAN Member
Port 01 02 03 04 05 06 07 08
PVID Selection
Port 09 10 11 12 13 14 15 16
PVID Selection
PVID Table
Port 01 02 03 04 05 06 07 08
VID --- --- --- --- --- --- --- ---
Port 09 10 11 12 13 14 15 16
VID --- --- --- --- --- --- --- ---
VLAN Member Table
VID
Port
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Figure 4-4

Multi to 1 Setting

Multi to 1 VLAN is used in CPE side of Ethernet-to-the-Home and is exclusive to VLAN setting on **VLAN Member Setting**. When VLAN member Setting is updated, multi to 1 setting will be void and vice versa. The disable port means the port which will be excluded in this setting. All ports excluded in this setting are treated as the same VLAN group. In a normal Tag Based VLAN network you will not need this configuration option.

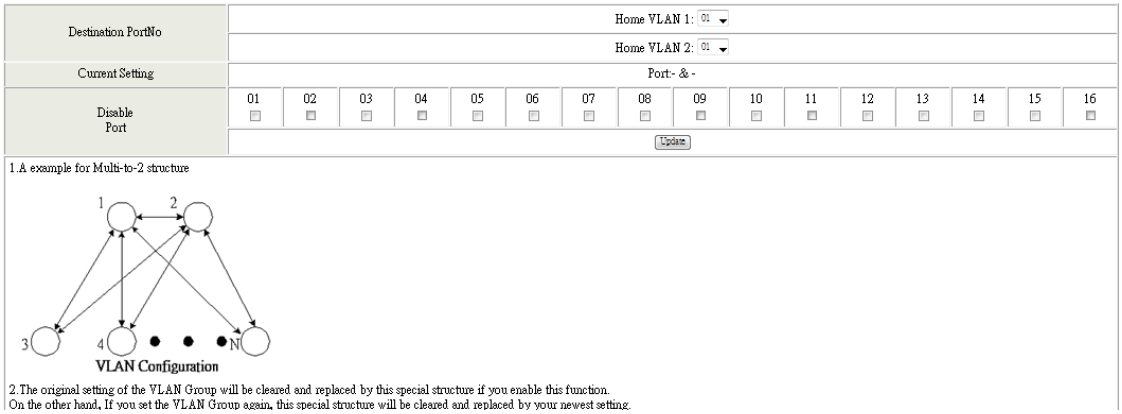

Destination PortNo
Home VLAN 1: 01
Home VLAN 2: 01
Current Setting
Port:- & -
Disable Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
Update
1.A example for Multi-to-2 structure
1
2
3
4
N
VLAN Configuration
2.The original setting of the VLAN Group will be cleared and replaced by this special structure if you enable this function.
On the other hand, If you set the VLAN Group again, this special structure will be cleared and replaced by your newest setting.

Figure 3-3

Per Port Counter

Port Counter

This page provides port counter of each port. There are 4 categories: Receive Packet & Transmit Packet/ Transmit & Collision / Receive Packet & Drop /Receive & CRC error. Once you change the counter category, the counter will be cleared automatically.

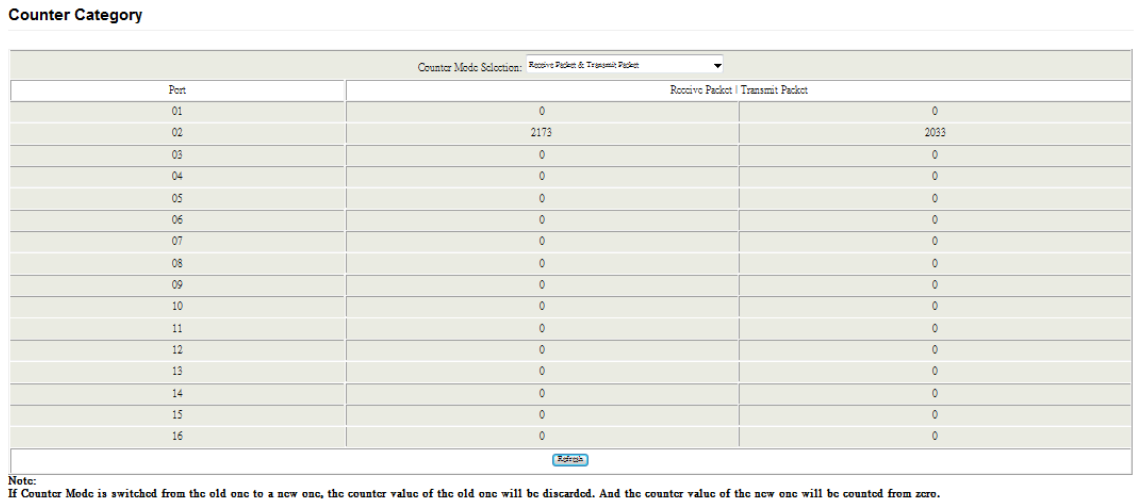

Counter Category
Counter Mode Selection:
Port
Receive Packet | Transmit Packet
01 0 0
02 2173 2033
03 0 0
04 0 0
05 0 0
06 0 0
07 0 0
08 0 0
09 0 0
10 0 0
11 0 0
12 0 0
13 0 0
14 0 0
15 0 0
16 0 0
Refresh
Note:
If Counter Mode is switched from the old one to a new one, the counter value of the old one will be discarded. And the counter value of the new one will be counted from zero.

Figure 5-1

- Transmit packet & Receive packet: This category shows both the received packet count (excluding the incorrect packet) and the transmitted packet count.
- Collision Count & Transmit packet: This category shows the packets outgoing from the switch and the count of collision.
- Drop packet & Receive packet: This category shows the number of received valid packet and the number of dropped packet.
- CRC packet & Receive packet: This category shows the received correct packet and received CRC error.
- Clear: Press “clear” will clear all counters.
- Refresh: Press “Refresh” button will aggregate the number of the counter for all ports.

QoS Setting

Here you can configure QoS policy priority mode and CoS (Class of Service) configuration. QoS (Quality of Service) refers to mechanisms in the network software that make the actual determination of which packets have priority. CoS refers to feature sets, or groups of services, that are assigned to users based on company policy. If a feature set includes priority transmission, then CoS winds up being implemented in QoS functions within the routers and switches in the network. In an enterprise network, class of service (CoS) differentiates high-priority traffic from lower-priority traffic. Tags may be added to the packets to identify such classes, but they do not guarantee delivery as do quality of service (QoS) functions, which are implemented in the network devices.

Priority Mode

There are three priority modes available to specify the priority of packets being serviced. Those include First-In-First-Out, All-High-Before-Low, and Weight-Round-Robin.

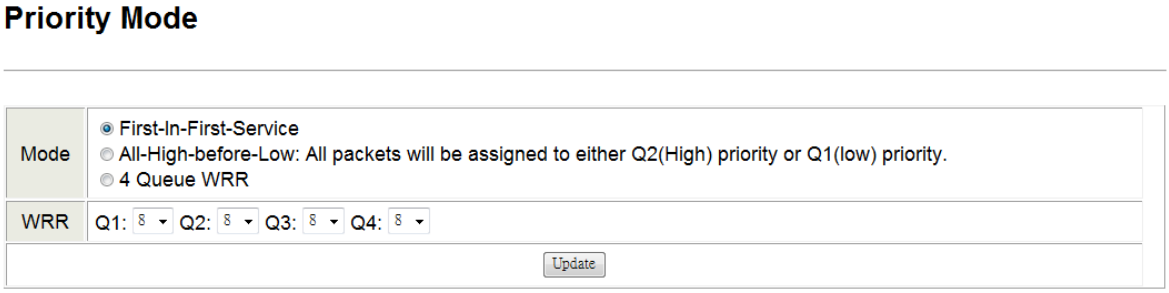


Figure 6-1

- First-In-First-Out: Packets are placed into the queue and serviced in the order they were received.
- All-high-before-low(Strict priority)：All packets will be assigned to either high priority queue (Queue 2) or low priority queue (Queue 1). The packet on the low priority queue will not be forwarded until the high priority queue is empty.
- WRR mode: There are 4 priority queues for Weighted-and-round-robin (WRR) mode. When this mode is selected, the traffic will be forwarded according to the number set in each queue.

Port, 802.1p, IP/DS based

Class of Service

The switch treats TCP/UDP, IP TOS/DS, 802.1p and physical port CoS scheme in the following priority.
TCP/UDP > IP TOS/DS > 802/1p > Physical port.
This means TCP/UDP CoS will override all other settings.

(1) TCP/UDP port

Protocol	**Note:** (1) Q1 ~ Q4 options are effective for the selected physical port only. (2) "Drop" option is the global setting for all physical ports.
FTP	Q1
SSH	Q1
TELNET	Q1
SMTP	Q1
DNS	Q1
TFTP	Q1
HTTP	Q1
POP3	Q1
NEWS	Q1
SNTP	Q1
NetBIOS	Q1
IMAP	Q1
SNMP	Q1
HTTPS	Q1
MSN	Q1
XRD_RDP	Q1
QQ	Q1
ICQ	Q1
Yahoo	Q1
BOOTP/ DHCP	Q1
User-defined A TCP/UDP	Q1
User-defined B TCP/UDP	Q1
User-defined C TCP/UDP	Q1

Note: These user-defined TCP/UDP port are the same as that used in TCP/UDP filter

User-defined Port range (65535~1)	User-defined A Port: ~ Port:	User-defined B Port: ~ Port:	User-defined C Port: ~ Port:

The TCP/UDP port will be checked on the following physical port

01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16

Update

The Class of Service for TCP/UDP port number allows the network administrator to assign the specific application to a priority queue.

(2) IP TOS/DS

IP TOS/DS Priority Setting	6'b001010: Q1 6'b010010: Q1 6'b011010: Q1 6'b100010: Q1 6'b101110: Q1 6'b110000: Q1 6'b111000: Q1 Other Values: Q1
IP TOS/DS Port Setting	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

Update

(3) 802.1p

For 802.1p priority field, the switch utilizes the following priority mapping table.
6 and 7 are mapped to the "Q4" priority queue.
4 and 5 are mapped to the "Q3" priority queue.
0 and 3 are mapped to the "Q2" priority queue.
1 and 2 are mapped to the "Q1" priority queue.

Port No\Mode	802.1p	Port No\Mode	802.1p
1		9	
2		10	
3		11	
4		12	
5		13	
6		14	
7		15	
8		16	

Update

(4) Physical port

1	Q1	9	Q1
2	Q1	10	Q1
3	Q1	11	Q1
4	Q1	12	Q1
5	Q1	13	Q1
6	Q1	14	Q1
7	Q1	15	Q1
8	Q1	16	Q1

Update

Figure 6-2

Security

MAC Address Binding

MAC Address Configuration

Port No.	MAC Address
1	: : : : : : : : : : : : : : : : : : Read
Select Port 01 Binding Disable Update	

Port No.	Filter Status	Port No.	Filter Status
1	Disable	9	Disable
2	Disable	10	Disable
3	Disable	11	Disable
4	Disable	12	Disable
5	Disable	13	Disable
6	Disable	14	Disable
7	Disable	15	Disable
8	Disable	16	Disable

Figure 7-1

- Port No: Displays the port number being assigned the MAC addresses.
- MAC Address: Users can assign up to 3 MAC addresses to the port.
- Read: Pull down the selection bar to choose a port number and click the read button to show the MAC addresses bound with the port or modify the MAC addresses.
- Select Port: Pull down the selection menu bar to choose a port number to be set.
- Binding: Enable or disable the binding function.

Click **Update** to have the configuration take effect.

TCP/UDP Filter

TCP/UDP Filter Configuration

Function Enable	Disable			
Port Filtering Rule	Deny "Deny" means the outgoing packets to the selected port with selected protocol will be dropped and other protocols will be forwarded. "Allow" means the selected protocol will be forwarded and other protocol will be dropped. Note: 1. The secure WAN port should be set at the physical port which is connected to the server. 2. Once this function is enabled, the switch will check the destination TCP/UDP port number at the outgoing direction of the secure WAN port. If the condition matches, this packet will be dropped or forwarded.			
Secure Port	Port01	Port02	Port03	Port04
	Port05	Port06	Port07	Port08
	Port09	Port10	Port11	Port12
	Port13	Port14	Port15	Port16
Protocol	FTP	SSH	TELNET	SMTP
	DNS	TFTP	HTTP	POP3
	NEWS	SNTP	NetBIOS	IMAP
	SNMP	HTTPS	XRD_RDP	BOOTP/ DHCP
	User-defined A TCP/UDP	User-defined B TCP/UDP	User-defined C TCP/UDP	
Update				

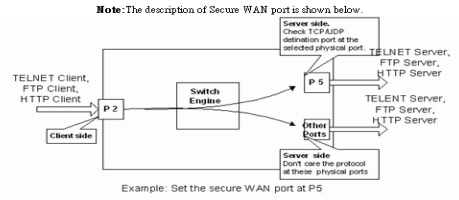

Note: The description of Secure WAN port is shown below.
Server side.
Check TCP/UDP
detination port at the
selected physical port.
TELNET Server,
FTP Server,
HTTP Server
TELNET Client,
FTP Client,
HTTP Client
P 2
Switch
Engine
P 5
TELENT Server,
FTP Server,
HTTP Server
Client side
Other
Ports
Server side
Don't care the protocol
at these physical ports
Example: Set the secure WAN port at P5

Figure 7-2

Spanning Tree

STP Bridge Settings

STP Bridge Settings

STP Bridge Status				
STP Mode	Bridge Priority (0~61440)	Hello Time (1~10 Sec)	Max Age (6~40 Sec)	Forward Delay (4~30 Sec)
		2	20	15
Submit				
Note: 2(Forward Delay-1) >= Max Age,* *Max Age >= 2*(Hello Time+1)*				

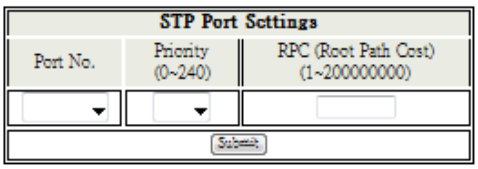
STP Bridge Status					
STP Mode	Bridge ID	Hello Time	Max Age	Forward Delay	Root ID
RSTP	32768:00 03 CE 01 21 DD	2	20	15	I'm the root bridge!

Figure 8-1

- Bridge Priority: This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 16 distinct values.
- Hello Time: Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1-10 (default is 2).
- Max Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6-40 (default is 20).
- Forward Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30 (default is 15)

STP Port Settings

STP Port Settings



STP Port Settings		
Port No.	Priority (0~240)	RPC (Root Path Cost) (1~200000000)
Submit		

STP Port Status						
Port No.	RPC	Priority	State	Status	Designated Bridge	Designated Port
1	6	0x80	--	Disable	--	--
2	14	0x80	Designated Port	Forwarding	--	--
3	1	0x80	--	Disable	--	--
4	3	0x80	--	Disable	--	--
5	15	0x80	--	Disable	--	--
6	10	0x80	--	Disable	--	--
7	1	0x80	--	Disable	--	--
8	15	0x80	--	Disable	--	--
9	10	0x00	--	Disable	--	--
10	2	0x00	--	Disable	--	--
11	Auto(200000)	0x00	--	Disable	--	--
12	Auto(200000)	0x00	--	Disable	--	--
13	Auto(200000)	0x00	--	Disable	--	--
14	Auto(200000)	0x00	--	Disable	--	--
15	Auto(200000)	0x00	--	Disable	--	--
16	Auto(200000)	0x00	--	Disable	--	--

Figure 8-2

- Port No: The port ID. It cannot be changed. Aggregations mean any configured trunk group.
- Root Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP path cost on the port. Number between 0 - 200000000. 0 means auto generated path cost.
- State: Show the current port state includes designated port, root port or blocked port.
- Status: Show the current port status includes forwarding, disable etc…

Loopback Detection Settings

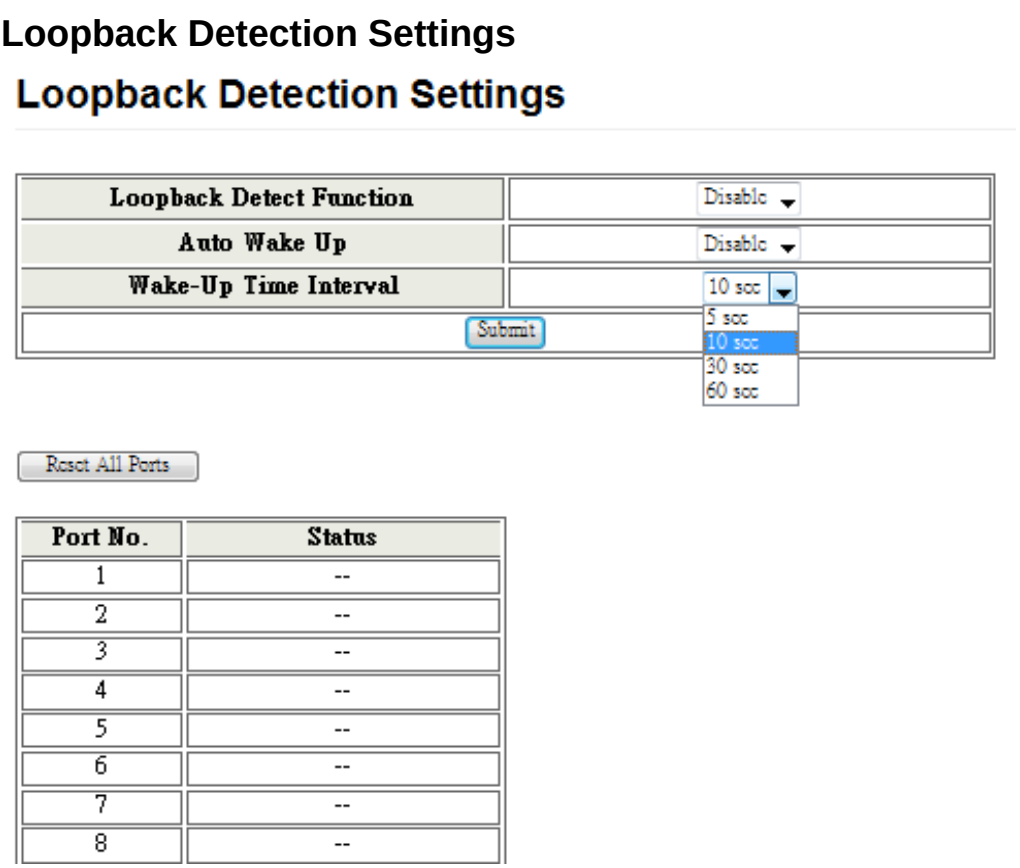


Figure 8-3

Trunking

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service. This switch may use Port ID, Source MAC Address, Destination MAC Address, or a combination of Source MAC Address and Destination MAC Address to be the selection for Trunk Hash Algorithm. Traffic pattern on the network should be considered carefully before applying it. When a proper hash algorithm is used, traffic is kind of randomly decided to be transmitted across either link within the trunk and load balancing will be seen.
This managed switch supports two trunk group, each trunk consists of 2~4 ports. Trunk hash algorithm can be selected according to 4 different methods.

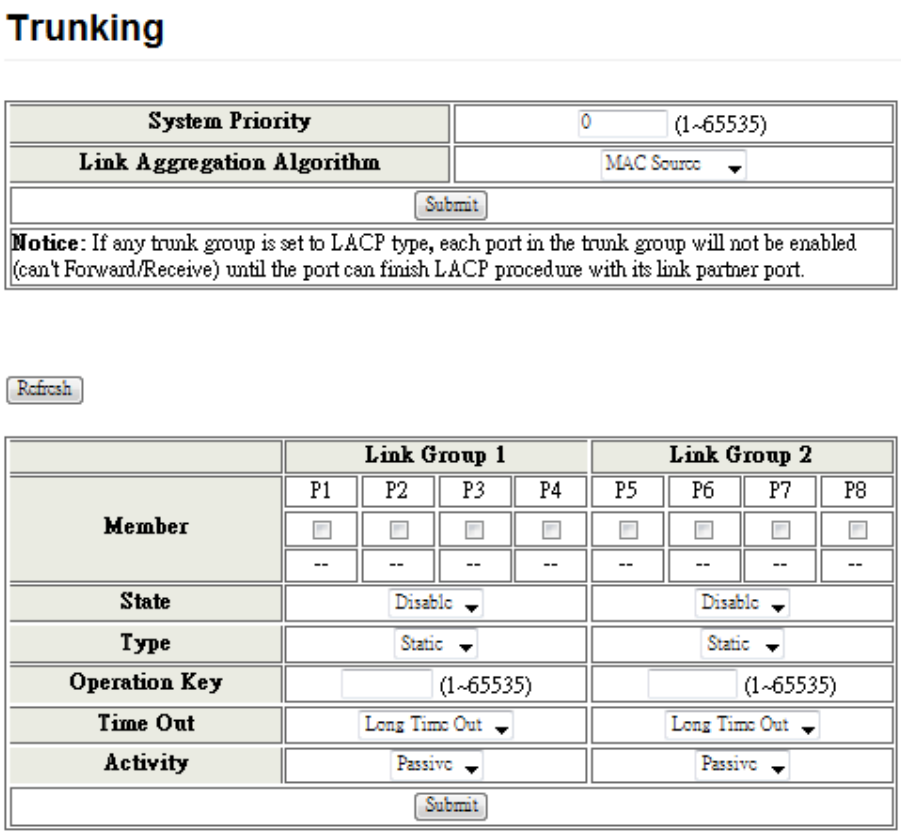


Figure 9-1

Backup/Recovery

This function provides the user with a method to backup/recovery the switch configuration. The user can save configuration file to a specified file. If the user wants to recover the original configuration, which is saved at the specified path, just enter the password and then press the “upload” button. Finally the original configuration of the switch will be recovered.

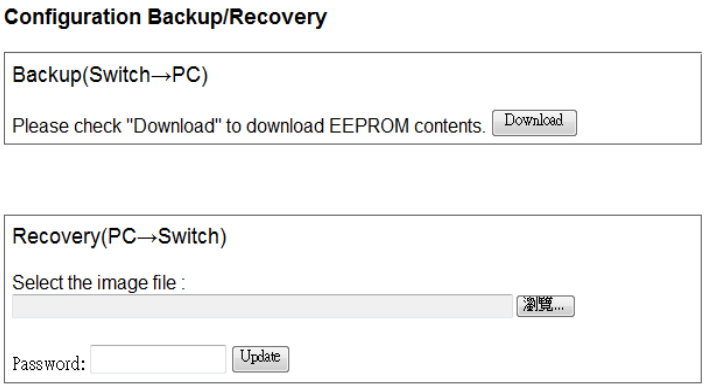


Figure 10-1

Miscellaneous

Miscellaneous setting is used to configure output queue aging time, VLAN stride and IGMP snooping.

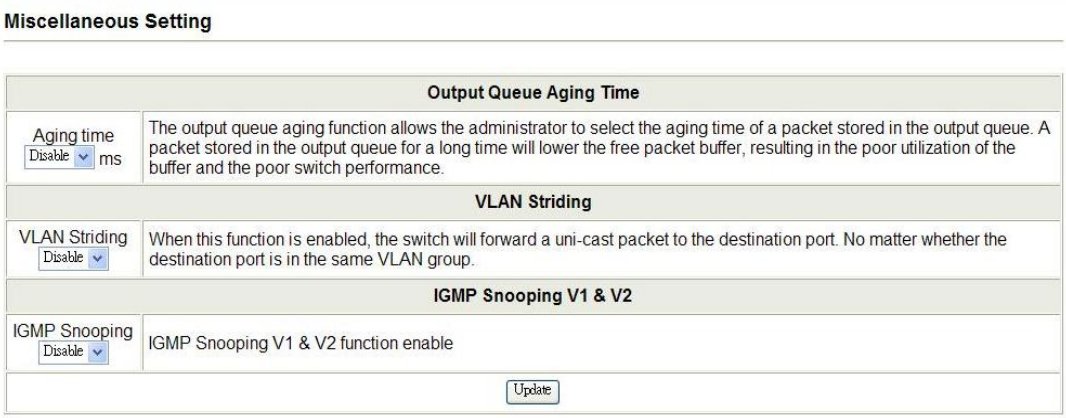

Miscellaneous Setting
Output Queue Aging Time
Aging time
Disable
ms
The output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long time will lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.
VLAN Striding
VLAN Striding
Disable
When this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.
IGMP Snooping V1 & V2
IGMP Snooping
Disable
IGMP Snooping V1 & V2 function enable
Update

Figure 11-1

- Output queue aging: This function is used to avoid the poor utilization of the switch. When a packet is stored in a switch for a long time, it will expire from the allowable time defined by the protocol and become a useless packet. To prevent these packets from wasting the bandwidth, this switch provide an option for the administrator to enable the queue aging function.
- VLAN Striding: By selecting this function, the switch will forward uni-cast packets to the destination port, no matter whether destination port is in the same VLAN.
- IGMP Snooping: When this function is enabled, the switch will execute IGMP snooping version 1 and version 2 without the intervention of CPU. The IGMP report and leave packets are automatically handled by the switch.

Logout

The administrator has write access for all parameters governing the onboard agent. User should therefore assign a new administrator password as soon as possible, and store it in a safe place.

When you forgot your IP or password, please use the reset button for the factory default setting?

Please take the following steps to reset the Web Smart Switch back to the original default:

Step 1:
Turn on the Web Smart Switch

Step 2:
Press and hold the reset button continuously for 5 seconds and release the reset button.

Step 3:
The switch will reboot for 20 seconds and the configuration of switch will back to the default setting.

Figure 12-1

Key in the user ID and the password to pass the authentication; the user ID and the password are “admin”

IP: 192.168.2.100
ID: admin
Password: admin